Factorization of integers and arithmetic functions

LINCOLN DURST

ABSTRACT

Elementary proofs of unique factorization in rings of arithmetic functions using a simple variant of Euclid's proof for the fundamental theorem of arithmetic.

1. Introduction.

In *The Elements* [**11**, BOOKS VII and IX] Euclid proved that, except for the order in which the factors are written, positive integers greater than 1 can be expressed uniquely as a product of *irreducible* integers p.

Euclid's argument has two main components:

(1) Each *composite* integer ab, with $a > 1$, $b > 1$, has an irreducible factor p, i. e., a factor whose only divisors are 1 and p. [BOOK VII, PROPOSITIONS 31, 32]

(2) Every irreducible integer is a *prime*, i. e., if p is irreducible, $ab > 1$, and $p \mid ab$, then $p \mid a$ or $p \mid b$. [VII, 20 and IX, 14]

Euclid or Euclid's translators introduced the expression prime number to represent what may be referred to in terminology of twentieth century algebra as an irreducible positive integer. Euclid deserves full credit, of course, for recognizing that irreducible positive integers have the more important property described in (2).

The need for a distinction between irreducibles and primes arose early in the nineteenth century when an impasse was encountered while attempting to prove Fermat's Last Theorem, since Euclid's (2) fails to hold in some rings where (1) holds, especially in cases involving real or complex algebraic numbers. See Edwards [**10**], Hardy and Wright [**12**], and Jacobson [**14**].

2. Euclid's original arguments.

For Euclid all integers are positive — and ordered, indeed well ordered, meaning no sequence of positive integers in which each member is less than its predecessor can be an infinite sequence, but must terminate after finitely many terms.

Here we are interested in factorization in a family of rings due to Liouville that are not ordered. First we modify Euclid's method,

using simple algebraic concepts, to reduce its dependence on the order relation Euclid used. Our variant of Euclid's (1) allows us to preserve Euclid's (2). Unlike the Fermat case, our procedure allows us to use only rational integers. In this sense our argument remains entirely elementary.

Euclid begins BOOK VII with a list of definitions, the relevant part here being that numbers larger than one must be *irreducible* or *composite*. The former have only trivial, i. e., unit, proper divisors; the latter have nonunit proper divisors.

Euclid's argument for property (1): If a and b are more than one, ab is composite. If a is irreducible, then ab has an irreducible factor. Otherwise a is composite, so some c divides a. If c is composite we repeat the previous step and begin generating a chain of proper divisors of ab. We must encounter an irreducible factor, for the only alternative is to generate an infinite sequence of divisors, each a proper divisor of its predecessor, and that is impossible. [**11**, vol. 2, p. 332]

Euclid has two proofs for (2): FIRST. If $p \,|\, ab$, then $pc = ab$ and $p : b = a : c$, i. e., $p/b = a/c$. If p does not divide b, the only common divisor of p and b is 1, so the ratio $p : b$ is in lowest terms and $m \geq 1$ exists with $a = mp$, $c = mb$, hence $p \,|\, a$. [**11**, vol. 2, p. 321]

SECOND. Let a be the least number divisible by all the irreducibles $p_1, p_2, \ldots, p_k$. Suppose q is an irreducible distinct from each of $p_1, p_2, \ldots, p_k$, and assume q divides a. Then $a = qm$. Since q does not equal any of $p_1, p_2 \ldots, p_k$, all the p_i must divide m. Because m is a proper divisor of a, this contradicts the minimal property of a. [**11**, vol. 2, p. 402]

Repeated use of (1) replaces each composite factor in a product by a product of irreducible factors. Thus one representation as a product of irreducibles is possible. Two such representations, involving different sets of irreducibles are not possible, as (2) shows. Note that one irreducible positive integer divides another only if they are equal since the only divisors of each are 1 and itself.

3. A variant of Euclid's argument.

A set is said to be *linearly ordered*, or to be a *chain*, if, given any pair, a, b, of distinct members, $a \neq b$, one is greater than the other: $a < b$ or $b < a$. A set is said to be *well ordered* if it is linearly ordered and if each of its nonvoid subsets contains a *least* element: one less than all other members of the subset. In addition to the set of positive integers, every finite linearly ordered set is well ordered.

No set of rational numbers, with their usual order, that contains the reciprocals of all the positive integers is well ordered. Examples: all the rationals, the real numbers, and complex numbers.

The argument we consider here involves a few simple concepts from twentieth century algebra: rings, semigroups, partially ordered sets, and chains of divisors.

If I is the ring of integers, I' the set of nonzero integers, and S the set of positive integers, the last two are examples of *semigroups* whose products are associative and commutative, and each contains the identity element 1 for the products in I. Since I is an integral domain, these semigroups are *cancellative*: $xy = xz$ implies $y = z$.

In any ring or semigroup, we define a *divides* b, or $a \mid b$, to mean the ring or semigroup contains a member c satisfying $ac = b$.

The difference between a group and a semigroup is the former contains the reciprocal of *each* of its members. In the two semigroups here, only 1, in S, and only ± 1, in I', divides *every* member of the semigroup, including the identity element. Members of rings or semigroups with this property are called *units*.

Possibly more esoteric than things mentioned so far, although surely simple as required here, are the MacKenzie *co-ideals* in a semigroup [**15**]:

DEFINITION. *If S is a commutative semigroup and $a \in S$, the subset $\{a\}$ of S containing all divisors of a is called a co-ideal of S.*

The relation $a \mid b$ is *reflexive*, since $a \mid a$ for all $a \in S$, and *transitive* since $a \mid b$ and $b \mid c$ imply $a \mid c$, for all $a, b, c \in S$; thus the relation $a \mid b$ shares two of the four defining properties of a 'weak' linear order relation, $a \leq b$. In the *special case* of the positive integers, it is also *antisymmetric*, since for each a, b,

$$a \mid b \text{ and } b \mid a \quad \text{imply} \quad a = b,$$

which corresponds to the linear order property

$$a \leq b \text{ and } b \leq a \quad \text{imply} \quad a = b.$$

The only other property of a linear order relation that $a \mid b$ lacks in general is, given any $a, b \in S$,

$$\text{either } a \leq b \text{ or } b \leq a, \quad \text{if } a \neq b.$$

A co-ideal $\{a\}$, is a finite subset of S, *partially ordered* by the divisor relation $x \mid y$ in S, that we may also write as $x \leq y$ using customary notation for a partial order relation.

As partially ordered sets, co-ideals can be represented as the union of chains by a theorem of Dilworth [**6**, theorem 1.1]; for the finite case, sufficient here, see Tverberg [**18**].

Each x in such a chain is a proper divisor, $x < y$, of each y above it in the chain. These chains, being finite linearly ordered sets are well ordered, and S is said to satisfy the *divisor chain condition*.

In terminology for partially ordered sets, a is the universal (greatest) element of the co-ideal $\{a\}$ generated by a, and the identity element, 1, for products in the ring containing S is the null (least) element of $\{a\}$. In the following example, a is a square free integer and the co-ideal $\{a\}$ is a boolean algebra. In less special cases, co-ideals can have more complicated structures. [Cf. § 10, below.]

EXAMPLE: The co-ideal of the divisors of 30 has a total of 2^3 members and is the union of the following three chains.

$$1,\ 2,\ 6,\ 30; \quad 1,\ 3,\ 15,\ 30; \quad 1,\ 5,\ 10,\ 30.$$

The *atoms* of a co-ideal, i. e., members covering only the null element, are *irreducible* elements of S since 1 is their only proper divisor.

In a partially ordered set if either $a \leq b$ or $b \leq a$, a and b are called a *comparable pair*, otherwise a and b are called *noncomparable*. According to Dilworth's theorem involved here, a partially ordered set P can be decomposed into the union of k chains provided each subset of P with $k + 1$ elements contains a comparable pair.

The atoms in $\{a\}$ have the maximal number of noncomparable elements for $\{a\}$ and the number of chains is the same as the number of atoms.

Euclid need not have assumed well ordering of the positive integers themselves was essential for their factorization into products of irreducibles. Here we have found well ordering where it is needed, in chains of divisors of integers, which is just where Euclid used it.

Euclid's criterion (2), or something effectively equivalent to it, is essential for uniqueness of the representation of positive integers as products of irreducibles and is what rules out the possibility of obtaining distinct products that are equal, say,

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l, \quad p_i, q_j \text{ irreducibles},$$

where the intersection of the set of ps and the set of qs is empty.

4. Liouville rings of arithmetic functions. (F)

If F is the *field* of rational, real, or complex numbers, we consider rings of arithmetic functions, whose elements are sequences of members of F indexed by positive integers, and prove unique factorization for this family of rings. In § 9 we consider sequences of integers.

Let R be a commutative and associative ring defined as follows, see Dickson [**8**], Bell [**2**], and Apostol [**1**]:

(1) The elements of R are all sequences, indexed by the positive integers, whose members are elements of F. We write the sequences in the form $\alpha(n)$ where $n \in S$, α being an arbitrary function mapping the positive integers into the field F.

(2) Addition in R is defined simply as $(\alpha + \beta)(n) = \alpha(n) + \beta(n)$.

(3) The zero of R, i. e., the identity element for addition, is the constant sequence $\omega(n) = 0$, for all $n \in S$.

(4) Products in R are defined by the finite sums

$$(\alpha * \beta)(n) = \sum_{d\delta=n} \alpha(d)\beta(\delta),$$

where d, δ run through the positive integers satisfying $d\delta = n$.

(5) The identity element for products is the sequence defined by

$$\varepsilon(n) = 1 \text{ for } n = 1 \quad \text{and} \quad \varepsilon(n) = 0 \text{ for } n > 1.$$

Each R is an integral domain: if $\alpha, \beta \neq \omega$, then a, b exist with $\alpha(a)\beta(b) \neq 0$, and $\alpha(n)\beta(m) = 0$ for $n < a$, $m < b$; hence $(\alpha*\beta)(ab) = \alpha(a)\beta(b) \neq 0$, i. e., products of nonzero elements are not zero.

Familiar members of each of these rings are Euler's φ-function, the number of positive divisors of n, the sum of those divisors, etc.

The units in these rings are the divisors of ε. To find all units we suppose $\alpha \in R$, $(\alpha * \alpha')(n) = 1$ for $n = 1$, $(\alpha * \alpha')(n) = 0$ for $n > 1$, and solve for α'. Now with $\alpha(1) \in F$, and

$$\alpha(1)\alpha'(1) = 1,\ \alpha(1)\alpha'(2) + \alpha(2)\alpha'(1) = 0,\ \alpha(1)\alpha'(3) + \cdots = 0, \ldots,$$

we *must* assume $\alpha(1) \neq 0$; this infinite system of equations can then be solved recursively by induction for $\alpha'(1)$, $\alpha'(2)$, $\alpha'(3), \ldots$. The solution is unique since the coefficient matrix of the first n equations is triangular and all elements on the diagonal are $\alpha(1)$. See Bell [**3**].

Thus all functions α with $\alpha(1) \neq 0$ are *units* in R, and *only* these. Observe that the sequences α in R that are units in R have

initial terms $\alpha(1)$ that are units in the underlying field F: every nonzero element d in a field is a unit since it divides 1, its cofactor being its reciprocal: $dd^{-1} = 1$. In R, all multiplicative functions have $\alpha(1) = 1$. Therefore the most familiar members of R, being units, are of negligible interest when it comes to unique factorization.

Consider the nonzero nonunits, $\alpha(1) = 0$, in R; more precisely, for some $a > 1$, $\alpha(n) = 0$ for $n < a$ and $\alpha(a) \neq 0$. If α and β are such nonunits, $(\alpha * \beta)(1) = \alpha(1)\beta(1) = 0$. Also $(\alpha * \beta)(p) = \alpha(1)\beta(p) + \alpha(p)\beta(1) = 0$ for *every* prime number p. CONTRAPOSITIVE: Every nonzero nonunit that is *not* zero for one or more prime numbers p cannot be expressed as a product of two nonzero nonunits; it is an *irreducible element*.

Among irreducible elements of R: the characteristic function χ of any set of prime numbers, i. e., $\chi(n)$ is 1 if n prime, zero otherwise; $(\pi(n))^2$ or, if F is the real field, $\log n$, $\log(n!)$, $\log(n^n)$, etc.

Let us call a the *rank* of α if for $a > 1$, $\alpha(a) \neq 0$, and $\alpha(n) = 0$ when $n < a$. If β has rank b, then the rank of $\alpha * \beta$ is the least n for which $(a * b)(n) \neq 0$. Since $\alpha(a)\beta(b) \neq 0$, and $\alpha(d)\beta(\delta) = 0$ if $d < a$ or $\delta < b$, it follows that

$$(\alpha * \beta)(ab) = \sum_{d\delta = ab} \alpha(d)\beta(\delta) = \alpha(a)\beta(b)$$

and the rank of the Liouville product $\alpha * \beta$ is ab.

If we extend this definition of *rank* so that units have rank 1, it follows that the rank of a product $\alpha * \beta$, for α, β nonzero, is the product of the ranks of its factors. Except for the zero element ω, every sequence in R has finite rank.

Suppose α and β have the same rank q, that is $\alpha(q) \neq 0$, $\beta(q) \neq 0$, and $\alpha(r) = \beta(r) = 0$ for $1 \leq r < q$. It follows that α, β differ by a unit factor: assume $\alpha = \beta * \gamma$. By hypothesis

$$\alpha(q) = \sum_{rs = q} \beta(r)\gamma(s) = \beta(1)\gamma(q) + \cdots + \beta(q)\gamma(1) = \beta(q)\gamma(1).$$

But $\alpha(q) \neq 0$ and $\beta(q) \neq 0$ imply $\gamma(1) \neq 0$. If q is a prime, α and β are irreducible, q being the first prime for which both are not zero.

5. Co-ideals in Liouville rings. (F)

In Liouville rings we define division and divisors as before: $\alpha(n)$ *divides* $\beta(n)$ means $\alpha * \gamma = \beta$ for some $\gamma(n) \in R$. In these cases we write T for the semigroup of nonzero members of R.

Suppose $\{\alpha\}$ is the co-ideal of an arbitrary member $\alpha(n)$ of T; when $\alpha, \beta \in T$, if $\alpha|\beta$ then $\{\alpha\} \subseteq \{\beta\}$, and conversely. If $\{\alpha\} \subset \{\beta\}$, we call α a *proper divisor* of β. If $\alpha \mid \beta$ *and* $\beta \mid \alpha$, then $\{\alpha\} = \{\beta\}$ and conversely. In the latter case, we say α and β are *associates* and for this relation we write $\alpha \sim \beta$.

If $\alpha(n)$ is a unit, $\{\alpha\}$ contains all the units in T, since every unit, by virtue of dividing every member of T, divides α.

Clearly if δ is a unit and if $\alpha * \delta = \beta$, then $\alpha|\beta$ and, since δ is a unit, we also have $\beta|\alpha$ because $\beta * \delta' = \alpha$ where δ' is the reciprocal of δ; i. e., $\delta * \delta' = \varepsilon$. Thus if α and β differ by a unit factor, $\alpha \sim \beta$.

The relation $\alpha \sim \beta$ is at the very least an equivalence relation, i. e., it is reflexive, transitive, and symmetric:

Reflexivity: $\alpha = \varepsilon * \alpha$ (ε is a unit).

Transitivity: $\alpha = \delta_1 * \beta$ and $\beta = \delta_2 * \gamma$ imply $\alpha = \delta_1 * \delta_2 * \gamma$ ($\delta_1 * \delta_2$ is a unit, if δ_1 and δ_2 are units).

Symmetry: $\alpha \sim \beta$ implies $\beta \sim \alpha$: if δ is a unit and $\alpha * \delta = \beta$, then $\beta * \delta' = \alpha$ if $\delta * \delta' = \varepsilon$.

Congruence: $\alpha_1 \sim \alpha_2$ and $\beta_1 \sim \beta_2$ imply $\alpha_1 * \beta_1 \sim \alpha_2 * \beta_2$, since $\alpha_1 = \delta_1 * \alpha_2$ and $\beta_1 = \delta_2 * \beta_2$ imply $\alpha_1 * \beta_1 = (\delta_1 * \delta_2) * \alpha_2 * \beta_2$.

With the last property included, the equivalence relation shares an additional well-known property with congruence relations.

For $r \geq 1$ let $\nu_r(n) = 1$ if $n = r$ and $\nu_r(n) = 0$ if $n \neq r$. Since the functions in each class of associates have the same rank, each class contains one of the functions ν_r; and if p and q are equal or distinct positive integers, $\nu_p * \nu_q = \nu_{pq}$, i. e., $(\nu_p * \nu_q)(n) = \nu_{pq}(n)$ for $n \geq 1$.

6. Reduced semigroups of Liouville rings. (F)

The elements of T are all the nonzero members of R, including, along with each member α, all of its associates. Let $\overline{\alpha}$ be the equivalence class whose members are α and its associates. Thus the semigroup T is the union of all the classes $\overline{\alpha}$ for $\alpha \in T$, and if α and β are not associates, the intersection $\overline{\alpha} \cap \overline{\beta}$ is empty.

For simplicity, we resort to a *homomorphism*, i. e., a many-to-one mapping from a larger set to a smaller set; we need one that maps Liouville products in T into Liouville products in the collection $\overline{T}$ of its equivalence classes. Thus we can transfer attention to a semigroup whose *members* are the equivalence classes of T. We define Liouville products in the semigroup $\overline{T}$ of equivalence classes as follows.

Given classes $\overline{\alpha}$ and $\overline{\beta}$, we take one element from each class, say $\alpha_1 \in \overline{\alpha}$ and $\beta_1 \in \overline{\beta}$, and form their product $\alpha_1 * \beta_1$.

According to the congruence-condition in the previous section, the product $\alpha_1 * \beta_1$ is in the same class with every other product of the form $\alpha_2 * \beta_2$ where α_2 is *any* member of $\overline{\alpha}$, and β_2 is *any* member of $\overline{\beta}$. Since the class containing these products depends only on the classes used and not on the members multiplied, we define

$$\overline{\alpha} * \overline{\beta} \quad \text{to be} \quad \overline{\alpha * \beta}.$$

By shifting attention from T to $\overline{T}$ we obtain a major simplification: note, for one example, the equivalence class containing all the units of T is the identity element for the Liouville product in $\overline{T}$.

$\overline{T}$ is called the *reduced semigroup* of T.

7. Isomorphism of the reduced semigroups S and $\overline{T}$. (F)

We have seen the associates of α all have the same rank. So there is a one-one correspondence between classes of associates and the common rank of their members: $\overline{\alpha} \leftrightarrow a$, $\overline{\alpha} \in \overline{T}$, $a \in S$.

The co-ideals $\{a\}$ and $\{\overline{\alpha}\}$ are *isomorphic* as partially ordered sets, i. e., if $\overline{\alpha}$ in the latter co-ideal is paired with its rank a in the former co-ideal, the divisor relations correspond since $\overline{\beta} \,|\, \overline{\alpha}$ in $\overline{T}$ if and only if $b \,|\, a$ in S. Therefore the partially ordered sets $\{a\}$ and $\{\overline{\alpha}\}$ are identical, except for the alphabets used to describe them.

8. Factorization into irreducibles and its uniqueness. (F)

For $\overline{T}$ we argue as for S, with the result that factorization into finitely many irreducible equivalence classes is possible and unique.

Each irreducible equivalence class can be represented by an arbitrary member of the class and alternate representatives may be chosen if in each instance a compensating unit factor is introduced as well; moreover, no matter how many alternate choices are made, the resulting product of units is itself a unit.

Thus each composite function α, can be written as the product of a single unit and finitely many irreducible factors.

Hence factorization of the *elements* of R takes the form

$$\delta\, \pi_1\, \pi_2 \cdots \pi_k,$$

where δ is a unit and $\pi_1, \pi_2, \ldots, \pi_k$ are irreducible members of R, a representation that is unique, except for the order of the factors and replacement by associates of the factors present.

9. Special Case: The subring of sequences of integers. (I)

The first proof for unique factorization in a ring of arithmetic functions was carried out for the field of complex numbers, a special case of the family of fields (F) described above in § 4; see Cashwell and Everett [**4**]. These authors conjectured unique factorization should also hold for the ring of integer valued arithmetic functions and proved it soon after [**5**]. In both cases F and I their methods were transfinite.

We now consider the case of the Liouville ring of arithmetic functions with integral values and encounter no significant differences from our elementary proofs when the functions have values in a field.

For this special case, we observe first that integers form a subring of each field F considered before, and the ring of sequences of integers is a subring of each of the corresponding rings R. The argument presented in sections 4 through 8 can be carried out simply by restricting attention to sequences of integers.

There are two differences between the cases based on F and I.

One is the paucity of units: for sequences of integers units have $\alpha(1) = \pm 1$ instead of $\alpha(1) \neq 0$ as for fields. This difference is negligible, the homomorphism simply wipes it out.

The difference in what qualifies as a unit entails the other difference: there are more nonunits, indeed there is a new family of irreducible elements. Because the defining condition for units now is $|\alpha(1)| = 1$ instead of $\alpha(1) \neq 0$, the two kinds of nonunits are distinguished since they satisfy *either* $\alpha(1) = 0$ *or* $|\alpha(1)| \geq 2$.

The case $\alpha(1) = 0$ is common to the earlier cases and the integral case, and presents no novelty.

The case $|\alpha(1)| \geq 2$ is even simpler. Observe that if $\alpha(n) = \beta(n) * \gamma(n)$ for all $n \geq 1$ and if $|\alpha(1)| = |\beta(1)|$, then $\gamma(1) = \pm 1$ since $|\alpha(1)| = |\beta(1)| \cdot |\gamma(1)|$. These nonunit sequences have rank one, in the terminology of the previous cases, and their only divisors are associates and units; therefore they are irreducibles.

In spite of these differences, the variant of Euclid's argument goes through as for the fields F considered earlier.

10. Summary of criteria for unique factorization.

The Euclidean algorithm (*Elements*, VII, 1, 2), often considered in this context, is obtained by repeated subtraction, which is easy for positive integers because they are (well) ordered and the division algorithm is available; but not in R.

Gauss argues that if a prime number divides neither a nor b, it cannot divide their product; this is a version of Euclid's condition (2). Gauss proves it [**13**, II, 14, 15] using congruences, also based on division with remainder and difficult to achieve without an order relation.

Dirichlet, in his lectures [**9**, § 1.8] avoids GCDs and the division algorithm, and argues as follows. If p is irreducible, its only divisors are 1 and p, so p shares no other divisors with *any* number. Dirichlet's observation implies Gauss's version of Euclid's criterion (2), as an immediate consequence of the definition of irreducibles.

For the cases considered here the essential hypothesis is the divisor chain condition, and for this have co-ideals.

For proofs in I and R the following hypotheses are superfluous: the division algorithm, the Euclidean algorithm, Euclid's (2), and existence of GCDs. The more relevant of these come from the co-ideals and the definition of irreducibles.

Co-ideals are lattices: We claimed the co-ideal of divisors of 30 is a boolean algebra because 30 has no square divisors.

A boolean algebra is a distributive lattice with unique complements; its characteristic property is that it is isomorphic to the lattice of all subsets of some set. The co-ideal $\{30\}$ is isomorphic to the collection of all subsets of the set $\{2, 3, 5\}$, including both the empty subset and the full set representing the divisors 1 and 30.

If in a partially ordered set each pair of elements x, y has a greatest lower bound and a least upper bound in its partial order relation $x \leq y$, the partially ordered set is called a *lattice*; the GLB and LUB are called, respectively, the *meet* and *join* of x and y and are denoted by $x \wedge y$ and $x \vee y$.

If the partial order relation is the divisor relation $x \mid y$, $x \wedge y$ is the GCD of x and y and $x \vee y$ is their LCM. See Pólya and Szegő [**16**].

A lattice is *complemented* if (a) it contains a universal element and a null element, often denoted by I and O, respectively; and (b) if for each member x there is at least one member x' with the properties $x \wedge x' = O$ and $x \vee x' = I$. (c) If each x has exactly one complement x', the lattice is said to have *unique complements*.

A lattice is *distributive* if $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ holds for all its members x, y, z. A necessary and sufficient condition for distributivity is $x \wedge y = x \wedge z$ and $x \vee y = x \vee z$ imply $y = z$, Crawley and Dilworth [**6**, p. 21]. If the partial order is the divisor relation $x \mid y$ both of these assertions are properties of GCDs and LCMs. The necessary

and sufficient condition follows immediately from $(x, y)[x, y] = xy$ and also implies that *any* complements that exist are unique.

For the special case of the co-ideal $\{30\}$, the complementary pairs are $1' = 30$, $2' = 15$, $3' = 10$, $5' = 6$, and by symmetry, $30' = 1$, etc. It follows that the co-ideal $\{30\}$ is a boolean algebra.

The co-ideal $\{12\}$ is the union of the following pair of chains $\langle 1, 2, 4, 12\rangle$ and $\langle 1, 3, 6, 12\rangle$. Complementary pairs of elements are $1' = 12$, and $3' = 4$, but not 2 and 6 since $2 \wedge 6 = 2$ and $2 \vee 6 = 6$. Here 12 is not square free; it is divisible by the square of 2. For more on lattices, see Crawley and Dilworth [**6**, chapters 1, 2].

For earlier studies of Liouville rings see **4**, **5**, and **7**; these papers use transfinite methods. The full force of Dilworth's theorem does also; it is proved using Zorn's lemma.

For the relation between arithmetic functions and Dirichlet series, see Pólya and Szegő, [**16**]. Cashwell and Everett's articles are based on the fact that Dirichlet series may be represented as power series in infinitely many variables, one variable for each positive prime number. In 1913 Harald Bohr published a study of the analytic properties of this pair of series representations in *Göttinger Nachrichten*, pages 444 – 488 [Reprinted as Item A 9, in volume one of Bohr's *Collected Mathematical Works*, København (1952)].

The product $*$ in R is often called Dirichlet convolution: see Apostol [**1**, § 2.14] and Popken [**17**].

References

1 Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer (1976). Chapter 2.

2 Eric Temple Bell, Abstract #4, *Bulletin of the American Mathematical Society*, **19** (1913), 166 – 167.

3 Eric Temple Bell, The reciprocal of a numerical function, *Tohoku Mathematical Journal*, **43** (1937), 77 – 78.

4 E. D. Cashwell and C. J. Everett, The ring of number-theoretic functions, *Pacific Journal of Mathematics*, **9** (1959), 975 – 985. Math. Revs. **21** (1960), p. 1334, #7226 (de Bruijn).

5 E. D. Cashwell and C. J. Everett, Formal power series, *Pacific Journal of Mathematics*, **13** (1963), 45 – 64. Math. Revs. **27** (1964), p. 1101, #5786.

6 Peter Crawley and Robert P. Dilworth, *Algebraic Theory of Lattices*, Prentice-Hall (1973).

7 Don Deckard and L. K. Durst, Unique factorization in power series rings and semigroups. *Pacific Journal of Mathematics*, **16** (1966), 239 – 242. Math. Revs. **32** (1966), p. 410, #2439.

8 Leonard Eugene Dickson, *History of the Theory of Numbers*, three volumes (1919), (1920), (1923). Carnegie Institution of Washington, publication 256. Reprinted Hafner (1934), Chelsea (1942). Vol. 1, pp. 285, 286.

9 P. G. L. Dirichlet, *Lectures on Number Theory*, History of Mathematics Sources **16**, American Mathematical Society/London Mathematical Society (1999).

10 Harold M. Edwards, *Fermat's Last Theorem*, Springer (1977). §§ 4.1, 4.2.

11 Euclid, *The Thirteen Books of The Elements*, translated with commentary by Sir Thomas L. Heath. Cambridge University Press, second edition (1926). Reprinted Dover (1956) and later.

12 G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford (1938). Fifth edition (1979). Chapter 14.

13 Carl Friedrich Gauss, *Disquisitiones Arithmeticæ*, English, Springer (1986).

14 Nathan Jacobson, *Basic Algebra I*, W. H. Freeman, 2nd. edition (1985). § 2.14.

15 Robert E. MacKenzie, Commutative semigroups. *Duke Mathematical Journal*, **21** (1959), 975 – 985.

16 George Pólya and Gabor Szegő, *Problems and Theorems in Analysis*, Springer, two volumes. First German ed. (1925), English (1978), (1976), reprinted (1998). Part VIII, §§ 1.4, 1.5.

17 Jan Popken, On convolutions in number theory, *Koninklijke Nederlandes Akademie van Wetenschappen*: Proceedings Series A. Mathematical Sciences (Amsterdam), **58** = *Indagationes Mathematicæ*, **17** (1955), 10 – 15.

18 Helge Tverberg, On Dilworth's decomposition theorem for partially ordered sets. *Journal of Combinatorial Theory*, **3** (1967), 305 – 306.

 `g_lkd@ams.org`